REMARKS

Claims 1-19 are currently pending in the application, of which claims 16-19 are newly added dependent claims. No new matter has been presented. Claims 1, 8, 10-12, and 14 are independent. Claim 10 incorporates the language of Claims 1 and 4, and Claim 11 incorporates the language of Claim 8. In the Office Action dated December 12, 2008, Claims 1, 3-8, and 10-12 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Pub. No. 2002/0108040 to Ahmet Eskicioglu ("Eskicioglu") in view of U.S. Patent No. 7,072,657 to Watanabe et al. ("Watanabe"). Additionally, Claim 14 was rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,289,102 to Ueda et al. ("Ueda") in view of Eskicioglu.

Applicants wish to extend their appreciation to the Examiner for the further indication that Claims 2, 9, 13, and 15 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims, as stated on page 9 of the Office Action dated December 12, 2008.

Regarding the rejection of independent Claims 1, 8, and 10-12, the Action dated December 12, 2008 alleges that Eskicioglu combined with Watanabe teaches every element of the claims. Applicants respectfully submit that the references cited fail to disclose or suggest the recited claims.

Eskicioglu appears to teach a cryptography scheme for providing conditional access to a received scrambled audio/visual (A/V) signal. Descrambling keys are generated using keys (shares) transmitted by a service provider and keys stored in a smart card [paragraph 0002]. As shown in Figure 1, the A/V signal is transmitted from the service provider(s) to the smart card, which is inserted into or coupled to a digital television [paragraphs 0031-0033]. The smart card is manufactured with keys already stored therein, as a 'prepositioned' shared secret scheme. These stored keys, along with an 'activating' key sent by the service provider, are used to reconstruct a scrambled signal from the service provider [paragraph 0038]. Since the stored keys are manufactured into the smart cards, modifying the scrambling key may be performed by changing the 'activating' key [paragraph 0044]. Subscribers in this conditional access system may be assigned different authorization levels by the different numbers of keys stored in their smart cards.

Various levels of smart cards allow access to certain programming, such as basic television (Level 1 smart card), premium channels (Level 2 smart card), or Pay-Per-View (Level 3 smart card) [paragraphs 0088-0093].

Regarding independent Claims 1, 8, 10, and 11, Applicants respectfully submit, among other teachings, Eskicioglu and Watanabe, individually or combined, fail to disclose or suggest "obtaining by a wireless station in advance an encryption key set including the differentiated encryption keys for the corresponding access points when initial authentication of the wireless station is performed" and/or "differentiated encryption keys provided to communicate data with corresponding access points," as recited in independent Claims 8 and 11, and similarly recited in independent Claims 1 and 10. In the Action dated December 18, 2008, page 3, it appears that paragraph 0038 of Eskicioglu is asserted as allegedly disclosing the above-cited portions of Claim 8. Applicants respectfully submit that it does not, and invite the Office to verify for itself the same after a careful review of Eskicioglu. Accordingly, it is submitted that a prima facie case of unpatentability is not established.

As noted above, Eskicioglu appears to teach in paragraph 0038 that a shared secret key is stored within both the transmitter (service provider) and the receiver (smart card). The smart card is manufactured with this shared secret key stored therein. Further, the smart card is merely used to reconstruct a symmetric key for descrambling a received A/V signal for display on a digital television [paragraph 0048]. As such, the above teaching by Eskicioglu is for a one-way communication system, there is no transmission from the receiver (smart card) to the transmitter (service provider). Applicants respectfully submit that the 'prepositioned' shared secret scheme used by Eskicioglu, which merely uses a shared key stored in both the transmitter and receiver, fails to disclose or suggest, for example, "obtaining by a wireless station in advance an encryption key set including the differentiated encryption keys for the corresponding access points when initial authentication of the wireless station is performed," as recited in independent Claims 8 and 11, and similarly recited in independent Claims 1 and 10.

Further, Eskicioglu appears to suggest that the principles of his teachings may be applied to "a method and apparatus for secure communications between a sender and receiver of information" [paragraph 0096]. However, Applicants respectfully submit that Eskicioglu provides

little or no support for this statement, much less any teaching or suggestion that to "differentiated encryption keys provided to communicate data with corresponding access points," as recited in independent Claims 8 and 11, and similarly recited in independent Claims 1 and 10.

Regarding independent Claim 12, Applicants respectfully submit, among other teachings, Eskicioglu fails to disclose or suggest "an access authorization determining unit for determining an access authorization class for communication between a wireless station and an access point" and/or "an encryption key allocation unit which reads an encryption key from the encryption key storing unit corresponding to a determination result of the access authorization determining unit and transfers a value of the encryption key to the wireless station," as recited in independent Claim 12. In the Action dated December 18, 2008, page 3, it appears that paragraph 0038 of Eskicioglu is asserted as allegedly disclosing the above-cited portions of Claim 12. Applicants respectfully submit that it does not, and invite the Office to verify for itself the same after a careful review of Eskicioglu. Accordingly, it is submitted that a prima facie case of unpatentability is not established.

As noted above with respect to, for example, Claims 1 and 8, Applicants respectfully submit that the 'prepositioned' shared secret scheme used by Eskicioglu, which merely uses a shared key stored in both the transmitter and receiver, fails to disclose or suggest, for example, "an encryption key allocation unit which reads an encryption key from the encryption key storing unit corresponding to a determination result of the access authorization determining unit and transfers a value of the encryption key to the wireless station" (emphasis added), as recited in independent Claim 12.

As noted above with respect to Claims 1 and 8, Eskicioglu appears to suggest that the principles of his teachings may be applied to "a method and apparatus for secure communications between a sender and receiver of information" [paragraph 0096]. However, Applicants respectfully submit that Eskicioglu provides little or no support for this statement, much less any teaching or suggestion to "an access authorization determining unit for determining an access authorization class for communication between a wireless station and an access point" (emphasis added), as recited in independent Claim 12.

Applicants further submit that Watanabe does not cure the deficiencies of Eskicioglu. Watanabe appears to disclose a method of coordinating the handoff of a mobile carrier between a first access network and a second access network. The method includes attempting a hand-off from a first access network that the mobile carrier is currently operating within to a second access network, wherein the attempting includes authenticating at the hyper operator only that the user may have access to the second access network via a contract earlier established. (See Watanabe, for example: abstract; col. 5, lines 8-55; and col. 6, lines 60-65.)

Accordingly, it is submitted that a prima facie case of obviousness is not established.

Regarding the rejection of independent Claim 14, the Action dated December 12, 2008 alleges that Ueda combined with Eskicioglu teaches every element of the claim. Applicants respectfully submit that the references cited fail to disclose or suggest the recited claims.

Ueda appears to teach a method for protecting data stored on a recording means such as a disk, e.g. a CD-ROM (Compact Disk-Read Only Memory) or DVD (Digital Video Disk) (col. 1, lines 18-52; col. 2, lines 43-60). Ueda attempts to prevent content recorded on the disk from being illegally copied, but not require a special data reading means to reproduce the data (col. 3, lines 34-42; col. 9, lines 23-29). First key information is recorded in a lead-in area and second key information is recorded in a data recording area. The first key may descramble the second key, while the second key may descramble the data. The first key may be encrypted by a master key (col. 3, line 51-col. 4, line 9). The disk can then be accessed only by a disk reproducing device, but other devices (such as a computer) cannot access the disk (col. 7, lines 25-39).

Applicants respectfully submit, among other teachings, Ueda and Eskicioglu, individually or combined, fail to disclose or suggest "A computer readable storage medium storing instructions which, when executed causes execution of a program implementing a structure of a wireless data packet in a wireless network that comprises a wireless station and an access point, the structure comprising: a header of said data packet transmitted through the wireless network" and/or "an access authorization information storing field, which indicated access authorization for communication between the wireless station and the access point," as recited in independent Claim 14. In the Action dated December 18, 2008, pages 7-8, it appears that Figures 1 and 13 of

Ueda are asserted as allegedly disclosing the first of above-cited portions of Claim 14. Applicants respectfully submit that they do not, and invite the Office to verify for itself the same after a careful review of Ueda. Accordingly, it is submitted that a prima facie case of unpatentability is not established.

As noted above, Ueda appears to teach a method of encrypting the data on an information recording medium, such as a disk. The encryption allows the recording medium to only be accessible by a disk reproducing device. There appears to be no teaching or suggestion of any wireless elements in Ueda. Therefore, Applicants respectfully submit that Ueda, which merely teaches encrypting data, fails to disclose or suggest, "A computer readable storage medium storing instructions which, when executed causes execution of a program implementing a structure of a wireless data packet in a wireless network that comprises a wireless station and an access point, the structure comprising: a header of said data packet transmitted through the wireless network" (emphasis added), as recited in independent Claim 14. As a first point, Ueda appears to only teach the storing of keys and data; thus there appears to be no disclosure or suggestion in Ueda to store instructions to be executed. As a second point, Ueda appears to only teach encrypting an information recording medium; there appears to be no disclosure or suggestion in Ueda for a wireless data packet, a wireless network, or "a header of said data packet transmitted through the wireless network".

In the Action dated December 18, 2007, page 8, it appears that paragraphs 0038, 0047, and 0088-0094 of Eskicioglu are asserted as allegedly disclosing the second of the above-cited portions of Claim 14, "an access authorization information storing field, which indicated access authorization for communication between the wireless station and the access point" (emphasis added). As noted above with respect to, for example, claims 1, 8, and 12, Eskicioglu appears to teach in paragraph 0038 that a shared secret key is stored within both the transmitter (service provider) and the receiver (smart card). The smart card is manufactured with this shared secret key stored therein. Further, the smart card is merely used to reconstruct a symmetric key for descrambling a received A/V signal for display on a digital television [paragraph 0048]. As such, the above teaching by Eskicioglu is for a one-way communication system, there is no transmission from the receiver (smart card) to the transmitter (service provider). Further, Eskicioglu appears to suggest that the principles of his teachings may be applied to "a method

and apparatus for secure communications between a sender and receiver of information" [paragraph 0096]. However, Applicants respectfully submit that Eskicioglu provides little or no support for this statement, much less any teaching or suggestion that is could be used in "an access authorization information storing field, which indicated access authorization for communication between the wireless station and the access point" (emphasis added), as recited in independent Claim 14. Applicants submit that Eskicioglu does not cure the deficiencies of Ueda. Accordingly, it is submitted that a prima facie case of obviousness is not established.

Because the above arguments put independent Claims 1, 8, 10-12 and 14 in condition for allowance, then, at least because of their dependence on these claims respectively, dependent Claims 2-7, 9, 13 and 15-19 are also in condition for allowance.

The application as now presented, containing Claims 1-15 are believed to be in condition for allowance. Early allowance of the same is respectfully solicited. Should the Examiner believe that a telephone conference or personal interview would facilitate resolution of any remaining matters or place any issue in better condition for Appeal, the Examiner may contact Applicants' representative at the number given below.

Respectfully submitted,

/Charles Y. Park/

Charles Y. Park
Reg No. 50,709

McNeely Bodendorf LLP
TEL: (202) 403-0802
FAX: (202) 478-1813

CYP:amd